Exam : CV0-003

Title : CompTIA Cloud+ Certification Exam

https://www.passcert.com/CV0-003.html

1.A company is concerned about the security of its data repository that contains customer PII. A systems administrator is asked to deploy a security control that will prevent the exfiltration of such data.
Which of the following should the systems administrator implement?
A. DLP
B. WAF
C. FIM
D. ADC
Answer: A
Explanation:
Reference:
https://cloud.google.com/blog/products/identity-security/4-steps-to-stop-data-exfiltration-with-google-cloud
Implementing DLP (Data Loss Prevention) is the best solution to prevent the exfiltration of customer PII (Personally Identifiable Information) from a data repository. DLP is a security control that monitors, detects, and blocks sensitive data from leaving or being accessed by unauthorized parties. DLP can be applied at different levels, such as network, endpoint, storage, or cloud. DLP can help to protect customer PII from being leaked, stolen, or compromised.

2.A web application has been configured to use autoscaling for provisioning and deprovisioning more VMs according to the workload. The systems administrator deployed a new CI/CD tool to automate new releases of the web application. During the night, a script was deployed and configured to be executed by the VMs during bootstrapping. Now. the autoscaling configuration is creating a new VM ever\ five minutes.
Which of the following actions will MOS I like y resolve the issue?
A. Reducing the maximum threshold in the autoscaling configuration
B. Debugging the script and redeploying it
C. Changing the automation tool because it is incompatible
D. Modifying the script to shut down the VM after five minutes
Answer: B
Explanation:
The best way to resolve the issue where the autoscaling configuration is creating a new VM every five minutes after deploying a new CI/CD tool to automate new releases of the web application and configuring a script to be executed by the VMs during bootstrapping is to debug the script and redeploy it. Debugging the script means finding and fixing any errors or bugs in the code or logic of the script that may cause unexpected or undesired behavior, such as triggering the autoscaling condition or failing to complete the bootstrapping process. Redeploying the script means updating or replacing the existing script with the corrected or improved version of the script.
Reference: [CompTIA Cloud+ Certification Exam Objectives], Domain 4.0 Troubleshooting, Objective 4.5 Given a scenario, troubleshoot automation/orchestration issues.

3.A security audit related to confidentiality controls found the following transactions occurring in the system:
GET http://gateway.securetransaction.com/privileged/api/v1/changeResource?id=123&user=277
Which of the following solutions will solve the audit finding?
A. Using a TLS-protected API endpoint

B. Implementing a software firewall
C. Deploying a HIDS on each system
D. Implementing a Layer 4 load balancer
Answer: A
Explanation:
Reference:
https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet .html
The audit finding is related to confidentiality, which means the data should be protected from unauthorized access. The current API endpoint is using HTTP, which is not secure and can expose the data in transit. Using a TLS-protected API endpoint would encrypt the data and prevent anyone from reading it.
Reference: CompTIA Cloud+ Certification Exam Objectives, Domain 2.0 Security, Objective 2.1 Given a scenario, apply security configurations and compliance controls to meet cloud security requirements.

4.A systems administrator is configuring RAID for a new server. This server will host files for users and replicate to an identical server. While redundancy is necessary, the most important need is to maximize storage.
Which of the following RAID types should the administrator choose?
A. 5
B. 6
C. 10
D. 50
Answer: C
Explanation:
RAID 50 is a type of RAID level that combines RAID 5 and RAID 0 to create a nested RAID configuration. RAID 50 consists of two or more RAID 5 arrays that are striped together using RAID 0. RAID 50 can provide redundancy, fault tolerance, and high performance for large data sets. RAID 50 can also maximize storage, as it has a higher usable capacity than other RAID levels with similar features, such as RAID 6 or RAID 10. The administrator should choose RAID 50 to configure a new server that will host files for users and replicate to an identical server, as it can meet the needs of redundancy and storage maximization.
References: CompTIA Cloud+ Certification Exam Objectives, page 9, section 1.4

5.A systems administrator recently upgraded the processors in a web application host. Upon the next login, the administrator sees a new alert regarding the license being out of compliance.
Which of the following licensing models is the application MOST likely using?
A. Per device
B. Per user
C. Core-based
D. Volume-based
Answer: C
Explanation:
Core-based licensing is a type of licensing model that charges based on the number of processor cores in a system or server. Core-based licensing is often used by software vendors to align their pricing with the performance and capacity of modern hardware. Core-based licensing can also enable customers to

optimize their licensing costs by choosing the appropriate hardware configuration for their needs. Upgrading the processors in a web application host can affect the core-based licensing of the application, as it may increase the number of cores that need to be licensed. This can result in an alert regarding the license being out of compliance if the license is not updated accordingly. References: CompTIA Cloud+ Certification Exam Objectives, page 20, section 4.2
Reference:
https://download.microsoft.com/download/3/d/4/3d42bdc2-6725-4b29-b75a-a5b04179958b/percorelicensing_definitions_vlbrief.pdf

6.A cloud administrator has created a new asynchronous workflow lo deploy VMs to the cloud in bulk. When the workflow is tested for a single VM, it completes successfully. However, if the workflow is used to create 50 VMs at once, the job fails.
Which of the following is the MOST likely cause of the issue? (Choose two.)
A. Incorrect permissions
B. Insufficient storage
C. Billing issues with the cloud provider
D. No connectivity to the public cloud
E. Expired API token
F. Disabled autoscaling
Answer: B,E
Explanation:
The most likely causes of the issue where the new asynchronous workflow fails to create 50 VMs at once in the public cloud are insufficient storage and expired API token. Insufficient storage means that there is not enough disk space available in the public cloud to accommodate all the VMs that are being created simultaneously. This could result in errors or failures during the provisioning process. Expired API token means that the authentication credential that is used by the workflow to communicate with the public cloud service has expired or become invalid. This could result in errors or failures during the API calls or requests.
Reference: CompTIA Cloud+ Certification Exam Objectives, Domain 4.0 Troubleshooting, Objective 4.5 Given a scenario, troubleshoot automation/orchestration issues.

7.A cloud architect wants to minimize the risk of having systems administrators in an IaaS compute instance perform application code changes. The development group should be the only group allowed to modify files in the directory.
Which of the following will accomplish the desired objective?
A. Remove the file write permissions for the application service account.
B. Restrict the file write permissions to the development group only.
C. Add access to the fileshare for the systems administrator’s group.
D. Deny access to all development user accounts
Answer: B
Explanation:
File write permissions are permissions that control who can modify or delete files in a directory or system. Restricting the file write permissions to the development group only can help minimize the risk of having systems administrators in an IaaS compute instance perform application code changes, as it can prevent

anyone other than the development group from altering or removing any files in the directory where the application code is stored. Restricting the file write permissions can also help maintain consistency and integrity, as it can ensure that only authorized and qualified users can make changes to the application code. References: CompTIA Cloud+ Certification Exam Objectives, page 14, section 2.7

8.Which of the following definitions of serverless computing BEST explains how it is different from using VMs?
A. Serverless computing is a cloud-hosting service that utilizes infrastructure that is fully managed by the CSP.
B. Serverless computing uses predictable billing and offers lower costs than VM compute services.
C. Serverless computing is a scalable, highly available cloud service that uses SDN technologies.
D. Serverless computing allows developers to focus on writing code and organizations to focus on business.
Answer: D
Explanation:
This is the best definition of serverless computing that explains how it is
different from using VMs (Virtual Machines). Serverless computing is a cloud service model that provides customers with a platform to run applications or functions without having to manage or provision any underlying infrastructure or resources, such as servers, storage, network, OS, etc.
Serverless computing is different from using VMs in the following ways:
- Serverless computing allows developers to focus on writing code and organizations to focus on business, rather than spending time and effort on managing or scaling VMs or other infrastructure components.
- Serverless computing is event-driven and pay-per-use, which means that applications or functions are executed only when triggered by a specific event or request, and customers are charged only for the resources consumed during the execution time.
- Serverless computing is more scalable and flexible than using VMs, as it can automatically adjust the capacity and performance of applications or functions according to demand or workload, without requiring any manual intervention or configuration.

9.A systems administrator wants to restrict access to a set of sensitive files to a specific group of users. Which of the following will achieve the objective?
A. Add audit rules on the server
B. Configure data loss prevention in the environment
C. Change tine permissions and ownership of the files
D. Implement a HIPS solution on the host
Answer: C
Explanation:
The best way to restrict access to a set of sensitive files to a specific group of users is to change the file permissions and ownership of the files. File permissions and ownership are attributes that determine who can read, write, execute, or modify the files. By changing the file permissions and ownership, the systems administrator can grant or deny access to the files based on the user identity or group membership.
Reference: CompTIA Cloud+ Certification Exam Objectives, Domain 2.0 Security, Objective 2.3 Given a scenario, implement appropriate access control measures for a cloud environment.

10.A company is considering consolidating a number of physical machines into a virtual infrastructure that will be located at its main office.
The company has the following requirements:
- High-performance VMs
- More secure
- Has system independence
Which of the following is the BEST platform for the company to use?
A. Type 1 hypervisor
B. Type 2 hypervisor
C. Software application virtualization
D. Remote dedicated hosting
Answer: A
Explanation:
A type 1 hypervisor is what would best meet the requirements of high-performance VMs (Virtual Machines), more secure, and has system independence for a company that wants to move its environment from on premises to the cloud without vendor lock-in. A hypervisor is a software or hardware that allows multiple VMs to run on a single physical host or server.
A hypervisor can be classified into two types:
☞ Type 1 hypervisor: This is a hypervisor that runs directly on the hardware or bare metal of the host or server, without any underlying OS (Operating System). A type 1 hypervisor can provide benefits such as:
☞ Type 2 hypervisor: This is a hypervisor that runs on top of an OS of the host or server, as a software application or program. A type 2 hypervisor can provide benefits such as:

11.A systems administrator is performing upgrades to all the hypervisors in the environment.
Which of the following components of the hypervisors should be upgraded? (Choose two.)
A. The fabric interconnects
B. The virtual appliances
C. The firmware
D. The virtual machines
E. The baselines
F. The operating system
Answer: C,F
Explanation:
These are the components of the hypervisors that should be upgraded by the administrator who is performing upgrades to all the hypervisors in the environment. A hypervisor is a software or hardware that allows multiple VMs (Virtual Machines) to run on a single physical host or server.
A hypervisor consists of various components, such as:
☞ The firmware: This is the software that controls the basic functions and operations of the hardware or device. The firmware can affect the performance, compatibility, and security of the hypervisor and the VMs. The firmware should be upgraded to ensure that it supports the latest features and functions of the hardware or device, as well as fix any bugs or vulnerabilities.
☞ The operating system: This is the software that manages the resources and activities of the hypervisor and the VMs. The operating system can affect the functionality, reliability, and efficiency of the hypervisor

and the VMs. The operating system should be upgraded to ensure that it supports the latest applications and services of the hypervisor and the VMs, as well as improve stability and performance.

12.A technician just received the lessons learned from some recent data that was lost due to an on-premises file-server crash. The action point is to change the backup strategy to minimize manual intervention.
Which of the following is the BEST approach for the technician to implement?
A. Backup as a service
B. RAID 1
C. Long-term storage
D. New backup devices
Answer: A
Explanation:
Backup as a service (BaaS) is the best approach for changing the backup strategy to minimize manual intervention after a data loss due to an on-premises file-server crash. BaaS is a cloud-based service that provides backup and recovery solutions for customers' data and systems. BaaS can automate and simplify backup processes by using cloud storage, encryption, deduplication, compression, scheduling, etc., without requiring customers to purchase or maintain backup hardware or software.

13.A systems administrator has received an email from the virtualized environment's alarms indicating the memory was reaching full utilization. When logging in, the administrator notices that one out of a five-host cluster has a utilization of 500GB out of 512GB of RAM. The baseline utilization has been 300GB for that host.
Which of the following should the administrator check NEXT?
A. Storage array
B. Running applications
C. VM integrity
D. Allocated guest resources
Answer: D
Explanation:
Allocated guest resources is what the administrator should check next after receiving an email from the virtualized environment's alarms indicating the memory was reaching full utilization and noticing that one out of a five-host cluster has a utilization of 500GB out of 512GB of RAM. Allocated guest resources are the amount of resources or capacity that are assigned or reserved for each guest system or device within a host system or device. Allocated guest resources can affect performance and utilization of host system or device by determining how much resources or capacity are available or used by each guest system or device. Allocated guest resources should be checked next by comparing them with the actual usage or demand of each guest system or device, as well as identifying any overallocation or underallocation of resources that may cause inefficiency or wastage.